UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

UNITED STATES OF AMERICA	)	DOCKET NO. 5:15CR15-RLV
	)	
	)	
v.	)	
	)	
(1) STEVEN W. CHASE	)	
	)	

UNITED STATE'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS INDICTMENT

Now comes the United States of America, by and through Jill Westmoreland Rose, United States Attorney for the Western District of North Carolina, Cortney Randall, Assistant United States Attorney for said District, and Reginald E. Jones, Trial Attorney, and submits the following response opposing defendant Steven Chase's Motion to Dismiss. As discussed more fully below, Chase was identified and arrested prior to the government's seizure and subsequent brief operation of the "Playpen" child pornography website. As such, the government's brief operation of Playpen to deploy a court-authorized Network Investigative Technique ("NIT") and to conduct authorized monitoring of user communications in order to identify website users is unrelated to the conduct for which Chase is being prosecuted. For this reason alone, Chase's motion to dismiss is meritless and should be denied without the need for a hearing.

Further, Chase mischaracterizes the facts of the government's brief operation of Playpen and his motion to dismiss lacks support under Fourth Circuit precedent. Finally, no court has concluded that the government's conduct was outrageous despite similar

allegations raised by defendants who (unlike Chase) were actually identified as a result of the government's brief operation of the website and deployment of the NIT.

I. BACKGROUND

The charges in this case arise from Chase's role as creator and primary administrator of the Playpen child pornography website operating on the anonymous Tor network. The scale of child sexual exploitation on the website was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site also included forums for discussion for all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

Playpen operated on the anonymous Tor network. Tor was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. The Tor network—and the anonymity it provides—is a powerful tool for those who wish to share ideas and information, particularly those living in places where freedom of speech is not accorded the legal protection it is here. But this anonymity has a downside. The Tor network is a haven for criminal activity in general, and the online sexual exploitation of children in particular. *See Over 80 Percent of DarkWeb Visits Relate to Pedophilia, Study Finds*, WIRED MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relatepedophilia-study-finds/ (last visited November 13, 2015).

Use of the Tor network masks the user's actual Internet Protocol ("IP") address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers.[1] To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP address-based identification techniques used by law enforcement on the open Internet are not viable.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

[1] Additional information about Tor and how it works can be found at www.torproject.org.

A "hidden service" like Playpen is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find Playpen, a user had to first get the web address for it from another source—such as another Playpen user or online postings identifying Playpen's content and location. Accessing Playpen thus required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity occurring on Playpen, investigators faced a tremendous challenge when it came to identifying Playpen users. Because Tor conceals IP addresses, normal law enforcement tools for identifying Internet users would not work. So even if law enforcement managed to locate Playpen and its IP logs, traditional methods of identifying its users would have gone nowhere.

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined that the computer server that hosted Playpen was located at a web-hosting facility in North Carolina and that Chase was the administrator of the server. The FBI was subsequently able to determine that Chase was also the creator and primary administrator of Playpen. On February 18, 2015, Chase was charged in the Western District of North Carolina with engaging in a child exploitation enterprise, conspiracy to advertise child pornography, advertising child pornography, transporting child pornography, and possession of child pornography. On February 19, a search warrant

was executed at Chase's Naples, Florida residence. Upon entering the residence, FBI agents encountered Chase and soon thereafter observed a laptop powered on and connected to the Playpen website. Chase, the only occupant of the home, was subsequently arrested. The FBI seized, and subsequently searched the laptop, along with several other devices. A subsequent review of the evidence seized at Chase's residence revealed files containing the Playpen logo, bookmarked links of Playpen forums, and more than 8,900 images depicting child abusive/exploitative material stored on his devices.

After the defendant's arrest on February 20, 2015, FBI subsequently seized and assumed administrative control of the website – which had already been operating for six months – for approximately two weeks in order to deploy a court-authorized Network Investigative Technique (the "NIT") and to conduct court-authorized monitoring of user communications to identify Playpen's users.

In his motion to dismiss, Chase alleges that the government's brief continued operation of the website to identify users amounts to "outrageous government conduct," and therefore seeks dismissal of the Indictment. However, as previously articulated, Chase was identified and arrested prior to the government's seizure and subsequent brief operation of the "Playpen" child pornography website. As such, the government's brief operation of Playpen to deploy a court-authorized Network Investigative Technique ("NIT") and to conduct authorized monitoring of user communications in order to identify website users other than Chase is unrelated to the conduct for which Chase is being prosecuted. For this reason alone, Chase's motion to dismiss is meritless and should be denied.

Nevertheless, without conceding any merit to Chase's motion to dismiss, the government will briefly address, why, even if Chase had been identified as a result of the government's brief operation of Playpen and deployment of the NIT, his motion lacks support under Fourth Circuit precedent. The Fourth Circuit has established that a defendant alleging outrageous government conduct must demonstrate that the government has done something that shocks the court's conscience. This Chase cannot do.

II. LEGAL STANDARDS

In order to obtain dismissal for purported "outrageous government conduct," Chase must demonstrate that he suffered a constitutional due process violation that is "outrageous, not merely offensive." *United States v. Goodwin*, 854 F.2d 33, 37 (4th Cir. 1998). The Fourth Circuit has "never held in a specific case that the government has violated the defendant's due process rights through outrageous conduct." *United States v. Hasan*, 718 F.3d 338, 343 (4th Cir. 2013) (holding that law remains clear in the Fourth Circuit that 'outrageous conduct' doctrine survives in theory, but is highly circumscribed"). While other circuits have articulated a series of factors to guide an outrageousness inquiry, see e.g., *United States v. Black*, 733 F.3d 294, 303 (9th Cir. 2013), the Fourth Circuit has not set forth a comprehensive list. It has however consistently held that to provide relief, the doctrine requires conduct so outrageous as to shock the conscience of the court, which will only occur in rare cases. *United States v. Dyess*, 478 F.3d 224, 334 (4th Cir. 2007).

Government conduct is not outrageous just because it involves a sting operation in a child pornography investigation. In *Goodwin*, the government identified its targets by

answering advertisements apparently seeking child pornography and by using lists transmitted by the Customs Service of the names of persons to whom such material had been sent from overseas and subsequently seized. In affirming the district court's determination that the government's conduct did not violate Goodwin's due process rights, the Fourth Circuit emphasized that "outrageous" is not a label properly applied to conduct just because it is a sting operation. *Id* at 37. The court also held that the due process calculation must take into consideration the nature of the crime involved, noting that undercover operations provide a means by which participants in the clandestine child pornography industry can be detected. *Id*. The court ultimately concluded that the sting operation was "neither shocking nor offensive to traditional notions of fundamental fairness."

In *United States v. Osborne*, Osborne alleged that the government's conduct in placing an advertisement and conducting a sting operation to uncover violations of 18 U.S.C. Section 2252(a)(2) was so outrageous as to have violated his Fifth Amendment right to due process of law, and that this conduct induced him to violate the law and thus constituted entrapment. The Fourth Circuit rejected this argument concluding that, "given the abundant and lenient appellate precedent concerning constitutionally permissible government conduct in undercover operations, it is clear that the government's conduct in the sting operation involving the defendant is far from outrageous by constitutional standards." 935 F.2d 32, 37 (4th Cir. 1991).

III. ARGUMENT

Should the Court reach this issue, nothing to which Chase points comes even remotely close to a violation of his due process rights, let alone one that is so outrageous as to shock the conscience. The government briefly assumed control of the website Chase created in order to conduct court-authorized monitoring of user communications and deploy a court-authorized investigative technique to identify those users, who were hiding their identities via technological means. Chase may disagree with the methods the government used to catch others. That does not render the government's court-authorized investigative techniques outrageous. Accordingly, the Court should deny the motion.

A. The Government Played No Role in Creating the Crime for Which Chase is Being Prosecuted or Otherwise Encouraged His Criminal Conduct.

Chase created the Playpen website, not the government. Moreover, Chase had been administrating Playpen for months when the website was identified by law enforcement. Soon thereafter, Chase was identified and arrested prior to the government's seizure and subsequent brief operation of Playpen. The government therefore bore no responsibility for Chase's criminal conduct and the medium by which the government ultimately identified Chase existed before and completely apart from the government's subsequent role in briefly hosting and monitoring the website to identify its users.

This matters because courts have recognized that "outrageous" conduct is more likely to be found were the *government* fabricates the crime and then invites the *defendant* along for the ride. *See, e.g.*, *United States v. Mayer*, 503 F.3d 740, 754 (9th Cir. 2007) (finding no outrageous government conduct and noting that the defendant was the first to

broach the subject of traveling internationally to have sex with boys). That is clearly not the case here.

Further, the duration of the government's operation of Playpen was exceedingly brief: two weeks. Chase created and operated the website for months prior to being arrested and the FBI obtaining control of the server. Moreover, while briefly operating Playpen, the FBI did not post any images, videos, or links to child pornography on the website. Chase, along with Playpen users under investigation, were responsible for that content. While images, videos, and links posted by site users (both before the FBI assumed administrative control and after) generally remained available to site users for a limited time period, for reasons explained below, removing all of that content would have jeopardized the investigation and the opportunity to identify and locate the users who possessed, distributed, and accessed it.

Chase claims that law enforcement made no effort to curtail the redistribution of child pornography through Playpen or to determine whether images posted pertained to new, as opposed to known, images of child pornography. *See* Def. Mot to Dismiss at 14. He is incorrect and views the government's actions through an unduly narrow lens. While Playpen operated under FBI administrative control, law enforcement authorities with the FBI monitored all site postings, chat messages, and private messages continuously to comply with Title III monitoring requirements and to access and mitigate risk of imminent harm to children. In the event FBI Special Agents perceived a risk of imminent harm to a child, agents took actions to mitigate that risk and immediately forwarded available

identifying information, including NIT results, to the appropriate FBI office. Actions taken in any particular instance were tailored to the specific threat of harm.

B. The Government Played No Role in Enhancing or Improving the Functionality of the Website

Chase claims absent actual factual support that the government enhanced or improved the website's functionality. *See* Def. Mot to Dismiss at 15. He is incorrect. His argument appears to be related to a misunderstanding, or misinterpretation, regarding certain postings to the website. When the FBI first assumed administrative control of the Playpen website, it experienced connectivity issues for a few days. Such connectivity issues are typical of all Tor hidden services, and eventually resolved themselves. One posting attached to Chase's motion was made after the connectivity issues were resolved to reference the fact that the connectivity issues had resolved themselves. *See* Def. Ex. 3, p. 4.[2] In addition, the Playpen website included a file hosting service. That service was brought back online shortly after the website itself was brought back online. The second posting attached to Chase's motion simply commemorates that pre-existing portion of the site coming back online. No feature was added to the site. *See* Def. Ex. 3, p. 5.

Chase also claims that the FBI was responsible for an increase in traffic to the Playpen website. *See* Def. Mot to Dismiss at 9. Again, Chase is incorrect. As reflected in the warrant seeking authority to deploy a Network Investigative Technique on the site, FBI analysis of historical data seized from Playpen indicated an average of 11,000 unique users

[2] The reference in that posting to an "upgrade" from "token ring" to "ethernet" was nothing more than an ironic reference to old networking technology. "Token ring" refers to a networking technology from the 1980s. In actuality, the FBI did not "upgrade" anything.

visited the site over the course of a week. That average included information from the site's inception until its seizure – including from the time near the site's inception when there would have been fewer users than at the time of seizure, when the site included more users. In any event, FBI took no actions to increase the number of Playpen visitors.

C. The Government's Conduct Was Necessary Given the Anonymous Network Chase and Other Playpen Members Used When Advertising, Sharing, and Viewing Child pornography

Additionally and independently, the government disagrees with Chase's characterization of its involvement in the Playpen website. The investigative means the government undertook were necessary to combat the underground child pornography trade and, further, to root out those who hid in the shadows of the Internet to exploit children.

As the government explained to the judges who authorized the NIT and the Title III – and as those judges apparently agreed – the brief, continued operation of Playpen in order to deploy the NIT was necessary to identify individuals actively sharing child pornography. Playpen users used technology to conceal their identities and locations. They did not do so for fear of discovery of some lawful, if distasteful, pursuit. Rather, they sought a safe haven where they could share depictions of small children being raped, sodomized, beaten, humiliated, and victimized in nearly every conceivable fashion without fear of law enforcement intervention. But for the government's investigation, these offenders would have succeeded in remaining hidden. The government explained, in great detail, the problem it faced in identifying these criminals and why other investigative

alternatives were simply not likely to succeed. *See* Def. Ex. 1, p. 22-24, ¶¶ 29-32 and Gov. Ex. 1, p. 38-43, ¶¶ 63-75[3].

Chase also suggests that the government should have identified his fellow offenders using other means. *See* Def. Mot. to Dismiss at 21. His proposals, unsurprisingly, fail to account for the sort of advanced technical means that Playpen users employed. As the government explained in its application for the Title III authorization, for the NIT to have an opportunity to work, members had to be able to continue to access the website with as minimal an interruption in the operation of the site as possible. This was necessary to avoid creating suspicion that a law enforcement interdiction was taking place. The government and the signing judicial official recognized that interruptions in the service of the Playpen website would tip-off suspects that law enforcement infiltration was taking place.

To be sure, agents considered seizing Playpen and removing it from existence immediately. Doing so might have ended child pornography trafficking on Playpen, but it would have come at a great cost: squandering any hope of identifying and apprehending the offenders responsible for engaging in hands-on exploitation as well as identifying and prosecuting those users. In other words, while such a tactic might have answered the immediate issue of child pornography trafficking on Playpen, it would have done nothing to address the larger problem. For the same reason, the other investigative alternatives Chase claims would have been preferable—*e.g.*, allowing users to login, thus permitting the deployment of the NIT, but restrict users' ability to download images from the website,

[3] "Playpen" is referenced in the affidavits as "Website A."

or disabling portions of the site that contained child pornography while allowing users to navigate other portions of the site, *see* Def. Mot. to Dismiss at 14, would likely have tipped users off to the fact of law enforcement infiltration and thus prevented law enforcement from identifying them.

Numerous child pornography bulletin boards similar in structure and function to Playpen currently operate on the Tor network. Collectively, the bulletin boards contain hundreds of thousands of user accounts and tens of thousands of postings that facilitate access to a momentous stockpile of images and videos of child pornography. Law enforcement agents can view and document those websites, their contents, and the child pornography images and videos trafficked through them. Because they operate as Tor hidden services, however, the location of the computer servers hosting the websites, the locations and identities of their users who are perpetrating crimes against children, and their child victims, remain unknown. Moreover, utilizing an alternative means would have frustrated agents' attempts to obtain information that could help identify and rescue child victims from ongoing abuse.

Accordingly, it was the judgment of law enforcement that the seizure and continued operation of Playpen for a discrete period of time, paired with the deployment of a NIT and monitoring of user communications, was necessary and appropriate to identify Playpen users. Two federal judges authorized the means for implementing that investigation. Stopping the unlawful possession and dissemination of child pornography, and rescuing children from ongoing abuse and exploitation, requires more than merely shutting down a facility through which such materials are disseminated. It was imperative that law

enforcement authorities also identify and apprehend the perpetrators. Here, the FBI briefly assumed administrative control over an existing facility through which users were already posting and accessing child pornography to deploy a court-authorized investigative technique and engage in court-authorized monitoring of user communications. These tactics—designed to identify the perpetrators—were necessitated by the particular anonymizing technology deployed by the users of the site. Undoubtedly, the decision whether to simply shut down a website like Playpen or to allow it to continue operating was a difficult one for law enforcement, given that users would continue to be able to post and access child pornography. Here, that difficult decision, which was disclosed to two different judges, was amply justified by the particular facts of the investigation. To date, the resulting investigation has identified or recovered at least 38 children who were subject to sexual abuse and exploitation by site users. The strong rationale supporting this investigation counsels against any finding of outrageousness.

D. No Court Has Concluded that the Government's Conduct was Outrageous Despite Similar Allegations raised by Defendants who (unlike Chase) were Actually Identified as a Result of the Government's Brief Operation of the Website and Deployment of the NIT

Chase has largely piggy-backed on the arguments of defendants who were identified as a result of the government's brief operation of Playpen and deployment of the NIT who have characterized the government's conduct as "outrageous" and, consequently, sought the extraordinary remedy of dismissal. Notably, Chase did not identify a single Playpen case that resulted in dismissal of an indictment. He does not because he cannot. Simply put, no court has concluded that the government's conduct in this matter was outrageous.

To the government's knowledge, two courts have ruled upon a Playpen motion to dismiss for outrageous conduct to date, *United States v. Michaud*, CR15-5351RJB (W.D. Wash.) and *U.S. v. Chauvin*, CR15-265 (E.D. LA.). In *United States v. Michaud*, a case where a defendant was actually identified as a result of the government's brief operation of the website and deployment of the NIT, the district court denied the request to dismiss and offered a clear and succinct assessment:

> It is easy to argue, and, my gosh, we hear it in all kinds of cases, that the other side's position is outrageous. Well, you know, that's a high standard. From the standpoint of one who stands between the defendant and the government, and represents neither side, you look at what happened and look inward. I am not shocked by this. I did not find it outrageous.

To the extent that this Court reaches this issue, it should come to the same conclusion.

CONCLUSION

The Court should deny Chase's motion because the conduct about which he complains had nothing to do with the conduct for which he is charged. Should this Court reach this issue, however, the court should deny the motion in any event because Chase fails to point to any due process violation, let alone one that is so outrageous as to shock the conscience. The government's conduct in this investigation was court-authorized and specifically targeted to identify serious criminals using technology to obscure their identity while exploiting children. That conduct was neither inappropriate nor outrageous. That Chase disagrees with those methods is no reason to dismiss his Indictment.

RESPECTFULLY SUBMITTED, this the 1st day of September, 2016.

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

s/ Cortney S. Randall
Assistant United States Attorney
NC Bar Number: 31510
Attorney for the United States
United States Attorney's Office
227 West Trade Street, Suite 1650
Charlotte, North Carolina 28202
Telephone: 704.344.6222
Fax: 704.344.6629
E-mail: cortney.randall@usdoj.gov

s/ Reginald E. Jones
Trial Attorney
Mississippi Bar Number: 102806
Attorney for the United States
U.S. Department of Justice, Criminal Division
Child Exploitation and Obscenity Section
Telephone: 202.616.2807
Reginald.Jones4@usdoj.gov

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this day, September 1, 2016, the foregoing was duly served upon counsel for the defendant by electronic means via the Court's ECF system to:

Peter Adolf
Attorney for Defendant
Peter_Adolf@fd.org

s/ Cortney S. Randall
Assistant United States Attorney
NC Bar Number: 31510
Attorney for the United States
United States Attorney's Office
227 West Trade Street, Suite 1650
Charlotte, North Carolina 28202
Telephone: 704.344.6222
Fax: 704.344.6629
E-mail: cortney.randall@usdoj.gov

s/ Reginald E. Jones
Trial Attorney
Mississippi Bar Number: 102806
Attorney for the United States
U.S. Department of Justice, Criminal Division
Child Exploitation and Obscenity Section
Telephone: 202.616.2807
Reginald.Jones4@usdoj.gov